



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/069,176	06/13/2002	Tomoyuki Asano	SONY JP-180	1654

530 7590 03/06/2006

LERNER, DAVID, LITTENBERG,  
KRUMHOLZ & MENTLIK  
600 SOUTH AVENUE WEST  
WESTFIELD, NJ 07090

EXAMINER

SHAW, YIN CHEN

ART UNIT PAPER NUMBER

2135

DATE MAILED: 03/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 10/069,176	<b>Applicant(s)</b> ASANO ET AL.	
	<b>Examiner</b> Yin-Chen Shaw	<b>Art Unit</b> 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 13 June 2002.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 6/13/2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>02/2002-06/2004</u> . | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

1. Claims 1-33 have been submitted for examination.
2. Claims 1-33 have been examined and rejected.
3. Rejections of Independent claims are provided with detailed citations from the prior arts.

## **Claim Objections**

4. Claim 29 is objected to because of the following informalities:
  - a. The term, "said storage means", appears to be a typographical error. The reference to the storage means does not appear in the claim limitations. The correct term should be "said information processing device". For examining purpose, the claim would be treated with the suggested correct term. Appropriate correction is required.

## **Claim Rejections - 35 USC § 103**

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-3, 5-9, 11, 15-17, 19-23, 25, 29, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Itkis (U.S. Patent 6,880,081) and further in view of Harada et al. (U.S. Patent 6,687,683).

a. Referring to Claims 1 and 11:

As per Claim 1, Itkis discloses an information processing device for processing encrypted data, comprising:

means for holding a node key unique to each of a plurality of nodes forming a hierarchical tree structure, having a plurality of such information processing devices, operating as leaves, and a leaf key unique to each of said information processing devices [In a preferable implementation of the group assignments 20 as shown in FIG. 1, the group assignments 20 may be depicted as a tree in which each one of the plurality of authorized devices is represented by a leaf (lines 21-26, Col. 8). At level n, the leaf level, each group 100 is associated with a device 110 (lines 16-17, Col. 9 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2 (lines 41-44, Col. 9 and Fig. 2 from Itkis)]; and

means for executing encryption processing [It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a

**key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K (lines 41-46, Col. 9 from Itkis)];**

said means executing decryption processing of decrypting a key block formed as key storage data that can be decrypted using at least one of said node key and the leaf key to effect calculation processing of calculating a decrypting key used in decrypting the encrypted data **[Accompanying the content is a key block B (the key block can be assumed to include “media key” – e.g., the disc’s serial number, etc. (lines 51-53, Col. 1 from Itkis). B can be computed (by the content providers, after examining the pirate devices) in such a way that all non-compromised devices can compute K from B (lines 56-58, Col. 1 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K (lines 41-46, Col. 9 and Fig. 2 from Itkis). Where K is a content encryption key or any other useful key (lines 7-8, Col. 10 from Itkis). Thus, each device 110 need only perform one decryption operation in order to obtain K. It is**

**appreciated that a further, typically fixed number of decryption operations, as is well known in the art, may need to be performed in order to actually obtain protected content (lines 12-16, Col. 10 from Itkis)];**

**said means also effecting encrypting processing for encrypting the calculated decrypting key using a key unique to the information processing device [At level n, the leaf level, each group 100 is associated with a device 110 (lines 16-17, Col. 9 from Itkis). Where a key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K (lines 41-46, Col. 9 and Fig. 2 from Itkis)].**

**Itkis discloses the hardware component for performing the encryption, decryption, and storage processes [In a preferred embodiment of the present invention, an improved key distribution system is provided (lines 49-50, Col. 2 from Itkis). Each of the components of FIG. 1 is preferably implemented in a combination of software and computer hardware, as is well known in the art, and may include special purpose computer hardware, as is also well known in art, in order to increase efficiency of operation (lines 3-7, Col. 8 and Fig. 1). Individual components, described below, of the security element 120 may be implemented in hardware or in any**

**suitable combination of hardware and software, as is well known in the art (lines 5-8, Col. 11 and Fig. 4)].** However, Itkis does not expressly disclose the hardware containing: (1) the storage means and encryption processing means within the processing devices for holding the key information, executing encryption/decryption processing, and effecting the encrypting processing, (2) to store the encrypted decrypting key on the recording medium or in a storage area in said information processing device. However, Harada et al. disclose (1) the LSI component, which contains the encryption and decryption units for deriving key information and performing encryption/decryption processes with keys and the storage unit for holding the relevant key information **[The disk key creation unit 1218 creates a 64-bit disk key including the information on the memory card ID that has been given from the memory card ID obtaining unit 1230. Here, a disk key is key data common to all kinds of memory card that is recording medium. The disk key encryption unit 1220 encrypts the disk key that has been created by the disk key creation unit 1218 using one of the plurality of master keys 1219 that have been stored in the disk key encryption unit 1220 in advance. The disk key encryption unit 1220 continues to encrypt the same disk key using a different master key 1219 to create the same number**

of encryption disk keys as that of the master keys 1219, and outputs the created encryption disk keys to the recording unit 1240 in the memory card writer 1200. The title key creation unit 1221 creates an appropriate 64-bit title key and gives the created title key to the title key encryption unit 1222. Here, the title key indicates key data that can be set for each music content (lines 8-24, Col. 13 from Harada et al.). Meanwhile, the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221, and outputs the re-encrypted C2 content 40 to the recording unit 1240 (lines 29-34, Col. 13 and unit 1200 in Fig. 2 and 3 from Harada et al.), and (2) to store the encrypted decrypting key on a recording medium or in a storage area in said information processing device [The title key encryption unit 1222 encrypts the title key that has been created by the title key creation unit 1221 using the disk that has been created by the disk key creation unit 1218, and outputs the encrypted title key to the recording unit 1240. Meanwhile the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221, and outputs the re-



encrypted C2 content 40 to the recording unit 1240 (lines 25-34, Col. 13). Note that the recording unit 1240 records the audio data that has been transferred from the audio data encryption unit 1223 in an user accessible area in the memory card 1300 and the encrypted disk key and title key in a system area in the memory card 1300 that cannot be accessed by the user (lines 39-43, Col. 13 and Fig. 2 from Harada et al.)). Itkis and Harada et al. are analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Itkis with Harada et al. since one would have been motivated to provide a production protection system that enables contents to be recorded on a recording medium loaded on a player for replaying contents and the like in order to more intensively protect contents for sale, and enables one of encryption algorithms for distributing contents via the Internet and for recording contents on the recording medium not to be influenced by the decryption of the other one (lines 53-60, Col. 1 from Harada et al.). Therefore, it would have been obvious to combine Itkis and Harada et al. to obtain the invention as specified in claim 1.

Art Unit: 2135

As per Claim 11, it encompasses some limitations that are similar to those of Claim 1. Therefore, these limitations are rejected with the same rationale applied against Claim 1 above. In addition, Harada et al. disclose said encryption processing means storing the calculated decrypting key in a storage area in said information processing device in association with the identification information used for discriminating said data decrypted using said decrypting key **[the memory card ID obtaining unit 1230 obtains the memory card ID that is inherent information from the memory card 1300, and gives the obtained memory card ID to the disk key creation unit 1218. When receiving the recording allowance, the recording unit 1240 records that data that have been output from the disk key encryption unit 1220, the title key encryption unit 1222, and the audio data encryption unit 1223 on the memory card 1300 (line 67, Col. 12 and lines 1-7, Col. 13 from Harada et al.). Meanwhile, the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221 (lines 29-32, Col. 13 from Harada et al.)]**.

b. Referring to Claim 2 and 16:

As per Claim 2, Itkis and Harada et al. disclose the information processing device according to claim 1 wherein the key unique to

said information processing device is said leaf key unique to each information processing device **[(lines 16-17 and 43-48, Col. 9 and Fig. 2 from Itkis)]**.

As per Claim 16, the rejection of Claim 15 is incorporated. In addition, Claim 16 encompasses limitations that are similar to those of Claim 2. Therefore, it is rejected with the same rationale applied against Claim 2 above.

c. Referring to Claim 3:

As per Claim 3, Itkis and Harada et al. disclose the information processing device according to claim 1 wherein

said key block includes a renewal key for renewing a node key stored in said storage means and said decrypting key **[(lines 51-53, Col. 1 from Itkis)]**;

said renewal node key is encrypted using a key at least including the node key or the leaf key of a lower layer **[(lines 56-59, Col. 2, lines 9-10 and 54-58, Col. 3, and lines 49-56, Col. 9)]**;

said decrypting key is encrypted using said renewal node key **[(lines 58-60, Col. 2 from Itkis)]**; and

wherein means decrypts said renewal node key, using at least one of the node key or the leaf key as held by said storage means, to acquire said renewal node key **[(lines 56-62, Col. 1 from Itkis)]**; and

said calculating said decrypting key using the so acquired renewal node key **[(lines 55-59, Col. 1 and lines 7-18, Col. 10 from Itkis)]**. In addition, Harada et al. disclose the encryption processing means as in claim 1.

d. Referring to Claims 5 and 19:

As per Claim 5, Itkis and Harada et al. disclose the information processing device according to claim 1 wherein said encryption processing means stores said decrypting key, encrypted using the key unique to the information processing device **[(lines 54-59, Col. 3 and lines 43-48, Col. 9 from Itkis)]**, in association with the identification information unique to said information processing device **[(lines 7-11, Col. 10 from Itkis)]**.

As per Claim 19, the rejection of Claim 15 is incorporated. In addition, Claim 19 encompasses limitations that are similar to those of Claim 5. Therefore, it is rejected with the same rationale applied against Claim 5 above.

e. Referring to Claims 6 and 20:

As per Claim 6, Itkis and Harada et al. disclose the information processing device according to claim 1 wherein said encryption processing means stores said decrypting key, encrypted using the key unique to the information processing device, in association with the identification information of encrypted data decrypted

using said decrypting key **[(line 67, Col. 12 and lines 1-7 and 29-32 Col. 13 from Harada et al.)]**.

As per Claim 20, the rejection of Claim 15 is incorporated. In addition, Claim 20 encompasses limitations that are similar to those of Claim 6. Therefore, it is rejected with the same rationale applied against Claim 6 above.

f. Referring to Claims 7 and 21:

As per Claim 7, Itkis and Harada et al. disclose the information processing device according to claim 1 wherein said decrypting key is a content key for decrypting the encrypted data **[(lines 48-50, Col. 1 and lines 7-8, Col. 10 from Itkis)]**.

As per Claim 21, the rejection of Claim 15 is incorporated. In addition, Claim 21 encompasses limitations that are similar to those of Claim 7. Therefore, it is rejected with the same rationale applied against Claim 7 above.

g. Referring to Claims 8 and 22:

As per Claim 8, Itkis and Harada et al. disclose the information processing device according to claim 1 wherein said decrypting key is a media key used for decrypting encrypted data **[(lines 48-50, Col. 1, and lines 7-8, Col. 10 from Itkis)]** and is a key allocated to said recording medium **[(lines 25-34 and 39-43, Col.**

**13 from Harada et al.); where the title key is the (media) content key and is located in the recording medium].**

As per Claim 22, the rejection of Claim 15 is incorporated. In addition, Claim 22 encompasses limitations that are similar to those of Claim 8. Therefore, it is rejected with the same rationale applied against Claim 8 above.

h. Referring to Claims 9 and 23:

As per Claim 9, Itkis and Harada et al. disclose the information processing device according to claim 1 wherein said decrypting key is a key held in common with other information processing devices and is a master key used for decrypting the encrypted data [(lines 48-50, Col. 1, lines 7-8, Col. 10, and lines 44-48, Col. 9 from Itkis); **where K is always the key used for decrypting the content even it is encrypted by different versions of keys**].

As per Claim 23, the rejection of Claim 15 is incorporated. In addition, Claim 23 encompasses limitations that are similar to those of Claim 9. Therefore, it is rejected with the same rationale applied against Claim 9 above.

i. Referring to Claims 15 and 29:

As per Claim 15, Itkis discloses an information processing method used in an information processing device, there being a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices operating as leaves, and a leaf key unique to each of said information processing devices, comprising:

decrypting a key block formed as key storage data that can be decrypted using at least one of said node key and the leaf key held by said information processing device **[Accompanying the content is a key block B (the key block can be assumed to include "media key" – e.g., the disc's serial number, etc. (lines 51-53, Col. 1 from Itkis). B can be computed (by the content providers, after examining the pirate devices) in such a way that all non-compromised devices can compute K from B (lines 56-58, Col. 1 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K (lines 41-46, Col. 9 and Fig. 2 from Itkis). Where K is a content encryption key or any other useful key (lines 7-8, Col. 10 from Itkis). Thus, each device 110 need only perform one decryption operation in order to obtain K. It is**

**appreciated that a further, typically fixed number of decryption operations, as is well known in the art, may need to be performed in order to actually obtain protected content (lines 12-16, Col. 10 from Itkis)];**

calculating a decrypting key used in decrypting the encrypted data **[K may be typically be obtained from B in the present invention by a legitimate device in a single decryption operation (lines 58-60, Col. 2). Where K is a content encryption key or any other useful key (lines 7-8, Col. 10)];**

encrypting the calculated decrypting key using a key unique to the information processing device **[It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K (lines 41-46, Col. 9 from Itkis)].**

Itkis does not expressly disclose storing the encrypted decrypting key on a recording medium or in a storage area in said information processing method. However, Harada et al. disclose the encrypted decryption key, used for decrypting the content information, is stored on the recoding medium **[The title key encryption unit 1222 encrypts the title key that has been created by the title key creation unit 1221 using the disk that**



has been created by the disk key creation unit 1218, and outputs the encrypted title key to the recording unit 1240. Meanwhile the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221, and outputs the re-encrypted C2 content 40 to the recording unit 1240 (lines 25-34, Col. 13). Note that the recording unit 1240 records the audio data that has been transferred from the audio data encryption unit 1223 in an user accessible area in the memory card 1300 and the encrypted disk key and title key in a system area in the memory card 1300 that cannot be accessed by the user (lines 39-43, Col. 13 and Fig. 2)]. Itkis and Harada et al. are analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Itkis with Harada et al. since one would have been motivated to provide a production protection system that enables contents to be recorded on a recording medium loaded on a player for replaying contents and the like in order to more intensively protect contents for sale, and enables one of encryption algorithms for distributing contents via the Internet and for recording contents on the

recording medium not to be influenced by the decryption of the other one (lines 53-60, Col. 1 from Harada et al.). Therefore, it would have been obvious to combine Itkis and Harada et al. to obtain the invention as specified in claim 15.

As per Claim 29, it is a computer program claim corresponding to the method claim 15. Thus, it is rejected with the same rationale applied against Claim 15 above. In addition, Harada et al. disclose the computer program executed on an information processing device [**The personal computer 1100 is a personal computer that includes a CPU, a memory, a hard disk and the like and executes a program (lines 43-45, Col. 7 from Harada et al.)**].

j. Referring to Claim 17:

As per Claim 17, Itkis and Harada et al. disclose the information processing method according to claim 15 wherein said key block includes a renewal key for renewing a node key stored in said information processing device and said decrypting key **[(lines 51-53, Col. 1 from Itkis)]**;

said renewal node key is encrypted using a key at least including the node key or leaf key of a lower layer **[(lines 56-59, Col. 2, lines 9-10 and 54-58, Col. 3, and lines 49-56, Col. 9)]**;

said decrypting key is encrypted by said renewal node key **[(lines 58-60, Col. 2 from Itkis)];**

the decrypting processing of said key block being the processing of decrypting the renewal node key, using at least one of the node key and the leaf key as held by said information processing device, to acquire said renewal node key **[(lines 56-62, Col. 1 from Itkis)];** and

wherein said calculating processing of said decrypting key uses the so acquired renewal node key to calculate the decrypting key **[(lines 55-59, Col. 1 and lines 7-18, Col. 10 from Itkis)].**

k. Referring to Claims 25 and 31:

As per Claim 25, it encompasses some limitations that are similar to those of Claim 1. Therefore, these limitations are rejected with the same rationale applied against Claim 1 above. In addition, Harada et al. disclose storing the calculated decrypting key in a storage area in said information processing device in association with the identification information for discriminating said data decrypted using said decrypting key **[the memory card ID obtaining unit 1230 obtains the memory card ID that is inherent information from the memory card 1300, and gives the obtained memory card ID to the disk key creation unit 1218. When receiving the recording allowance, the recording unit 1240 records that data that have been output from the**

Art Unit: 2135

**disk key encryption unit 1220, the title key encryption unit 1222, and the audio data encryption unit 1223 on the memory card 1300 (line 67, Col. 12 and lines 1-7, Col. 13 from Harada et al.). Meanwhile, the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221 (lines 29-32, Col. 13 from Harada et al.).]**

As per Claims 31, it is a computer program claim corresponding to the method claim 25. Thus, it is rejected with the same rationale applied against Claim 25 above. In addition, Harada et al. disclose the computer program executed on an information processing device **[The personal computer 1100 is a personal computer that includes a CPU, a memory, a hard disk and the like and executes a program (lines 43-45, Col. 7 from Harada et al.).]**

6. Claims 4, 10, 18, 24, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Itkis (U.S. Patent 6,880,081) and Harada et al. (U.S. Patent 6,687,683) and further in view of Lotspiech et al. (U.S. Patent 6,118,873).

a. Referring to Claims 10:

Art Unit: 2135

As per Claim 10, it encompasses some limitations that are similar to those of Claim 1. Therefore, these limitations are rejected with the same rationale applied against Claim 1 above. Itkis and Harada et al. do not expressly disclose the decryption key is in association with the generation number as the renewal information for said decrypting key. However, Lotspiech et al. disclose the renewal generation number is associated with the number of the time the decryption key has been renewed **[the renewal generation number refers to the number of times the keys of a device have been renewed (lines 21-23, Col. 6 from Lotspiech et al.)]**. Itkis, Harada et al. and Lotspiech et al. are analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Itkis and Harada et al. with Lotspiech et al. since one would have been motivated to prevent the unauthorized viewing and/or copying (line 13, Col. 1 from Lotspiech et al.). Therefore, it would have been obvious to combine Itkis and Harada et al. with Lotspiech et al. to obtain the invention as specified in claim 10.

b. Referring to Claims 4 and 18:

As per Claim 4, Itkis and Harada et al. disclose the information processing device according to claim 1 wherein said encryption

processing means stores said decrypting key, encrypted using the key unique to the information processing device **[(lines 54-59, Col. 3 and lines 43-48, Col. 9 from Itkis)]**. Itkis and Harada et al. do not expressly disclose the decryption key is in association with the generation number as the renewal information for said decrypting key. However, Lotspiech et al. disclose the renewal generation number is associated with the number of the time the decryption key has been renewed **[(lines 21-23, Col. 6 from Lotspiech et al.)]**. Itkis, Harada et al. and Lotspiech et al. are analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Itkis and Harada et al. with Lotspiech et al. since one would have been motivated to prevent the unauthorized viewing and/or copying (line 13, Col. 1 from Lotspiech et al.). Therefore, it would have been obvious to combine Itkis and Harada et al. with Lotspiech et al. to obtain the invention as specified in claim 4.

As per Claim 18, the rejection of Claim 15 is incorporated. In addition, Claim 18 encompasses limitations that are similar to those of Claim 4. Therefore, it is rejected with the same rationale applied against Claim 4 above.

c. Referring to Claims 24 and 30:

As per Claim 24, it encompasses some limitations that are similar to those of Claim 15. Therefore, these limitations are rejected with the same rationale applied against Claim 15 above. Itkis and Harada et al. do not expressly disclose the decrypting key in a storage area in said information processing device is in association with the generation number as the renewal information for said decrypting key. However, Lotspiech et al. disclose the renewal generation number is associated with the number of the time the decryption key has been renewed **[the renewal generation number refers to the number of times the keys of a device have been renewed (lines 21-23, Col. 6 from Lotspiech et al.)]**. Itkis, Harada et al. and Lotspiech et al. are analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Itkis and Harada et al. with Lotspiech et al. since one would have been motivated to prevent the unauthorized viewing and/or copying (line 13, Col. 1 from Lotspiech et al.). Therefore, it would have been obvious to combine Itkis and Harada et al. with Lotspiech et al. to obtain the invention as specified in claim 24.

As per Claim 30, it is a computer program claim corresponding to the method claim 24. Thus, it is rejected with the same rationale applied against Claim 24 above.

7. Claims 12-14, 26-28, and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Itkis (U.S. Patent 6,880,081) and further in view of Harada et al. (U.S. Patent 6,687,683) and Tatebayashi (U.S. Patent 6,359,986).

a. Referring to Claim 12:

As per Claim 12, Itkis discloses an information processing device for processing encrypted data, comprising:

means for holding a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices as leaves, and a leaf key unique to each of said information processing devices [In a preferable implementation of the group assignments 20 as shown in FIG. 1, the group assignments 20 may be depicted as a tree in which each one of the plurality of authorized devices is represented by a leaf (lines 21-26, Col. 8). At level n, the leaf level, each group 100 is associated with a device 110 (lines 16-17, Col. 9 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to



each of the groups 100 of FIG. 2 (lines 41-44, Col. 9 and Fig. 2 from Itkis)); and

means for executing decrypting processing [Thus each device 110 need only perform one decryption operation in order to obtain K. It is appreciated that a further, typically fixed number of decryption operation, as is well known in the art, may need to be performed in order to actually obtain protected content (lines 12-16, Col. 10 from Itkis)];

to retrieve whether or not a decrypting key used for decrypting the encrypted data is stored therein [The content is distributed form, with K denoting the key used for the encryption (K could be a "key-encrypting-key") (lines 48-50, Col. 1). It is appreciated that a possibility is thus set up for the remainder of the method of FIG. 5 to determine whether the key with which the invalid content key is encrypted is know to the device (lines 47-50, Col. 12 from Itkis). It is further appreciated that a preferably goal of black box analysis is to produce a set of keys which pirate devices to not use for decoding protected content, but which are know to all valid devices (lines 28-31, Col. 13 from Itkis)];

said means effecting decrypting processing of the encrypted decrypting key, in case the decrypting key has been detected, to calculate the decrypting key used for decrypting the encrypted

data [performing no more than a predetermined number of decryption operations, the predetermined number being the same for all authorized devices, to obtain the content decryption key from an encrypted form thereof, the encrypted form being encrypted with a group key corresponding to a group of which the authorized device is a member (lines 54-59, Col. 3 from Itkis). A key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 670 are used, independently, to encrypt K (lines 43-46, Col. 9 from Itkis)];

said means effecting decrypting processing of a key block formed by decryptable key storage data, in case of failure in detecting the decrypting key, using at least one of the node key and the leaf key held by said storage means, to calculate the decrypting key used in decrypting the encrypted data [Accompanying the content is a key block B (the key block can be assumed to include "media key" – e.g., the disc's serial number, etc. (lines 51-53, Col. 1 from Itkis). B can be computed (by the content providers, after examining the pirate devices) in such a way that all non-compromised devices can compute K from B (lines 56-58, Col. 1 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to

each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K (lines 41-46, Col. 9 and Fig. 2 from Itkis). Where K is a content encryption key or any other useful key (lines 7-8, Col. 10 from Itkis). Thus, each device 110 need only perform one decryption operation in order to obtain K. It is appreciated that a further, typically fixed number of decryption operations, as is well known in the art, may need to be performed in order to actually obtain protected content (lines 12-16, Col. 10 from Itkis)].

Itkis discloses the hardware component for performing the encryption, decryption, and storage processes [In a preferred embodiment of the present invention, an improved key distribution system is provided (lines 49-50, Col. 2 from Itkis). Each of the components of FIG. 1 is preferably implemented in a combination of software and computer hardware, as is well known in the art, and may include special purpose computer hardware, as is also well known in art, in order to increase efficiency of operation (lines 3-7, Col. 8 and Fig. 1). Individual components, described below, of the security element 120 may be implemented in hardware or in any suitable combination of hardware and software, as is well known in the art (lines 5-8, Col. 11 and Fig. 4)]. However, Itkis

does not expressly disclose the hardware containing: (1) the storage means and decryption processing means within the processing devices for holding the key information, executing encryption/decryption processing, and effecting the decrypting processing, (2) reading in a table stored on a recording medium or in a recording area in the information processing device (3) the encrypted decrypting key stored on the recording medium or in the recording area in the information processing device.

However, Tatebayashi discloses (2) reading a table stored on the recording medium or in a storage area in an information processing device **[The encryption key set distribution unit 116 reads the first encryption key set 420 from the encryption key table 114 and writes it into a first encryption key set storage medium (lines 66-67, Col. 8 and line 1, Col. 9)].**

In addition, Harada et al. disclose (1) the LSI component, which contains the encryption and decryption units for deriving key information and performing encryption/decryption processes with keys and the storage unit for holding the relevant key information **[The disk key creation unit 1218 creates a 64-bit disk key including the information on the memory card ID that has been given from the memory card ID obtaining unit 1230. Here, a disk key is key data common to all kinds of memory card that is recording medium. The disk key encryption unit**

1220 encrypts the disk key that has been created by the disk key creation unit 1218 using one of the plurality of master keys 1219 that have been stored in the disk key encryption unit 1220 in advance. The disk key encryption unit 1220 continues to encrypt the same disk key using a different master key 1219 to create the same number of encryption disk keys as that of the master keys 1219, and outputs the created encryption disk keys to the recording unit 1240 in the memory card writer 1200. The title key creation unit 1221 creates an appropriate 64-bit title key and gives the created title key to the title key encryption unit 1222. Here, the title key indicates key data that can be set for each music content (lines 8-24, Col. 13 from Harada et al.). Meanwhile, the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221, and outputs the re-encrypted C2 content 40 to the recording unit 1240 (lines 29-34, Col. 13 and unit 1200 in Fig. 2 and 3 from Harada et al.)), and (3) the encrypted decrypting key stored on a recording medium or in a storage area in said information processing device [The title key encryption unit 1222 encrypts the title key that has been created by the title key creation unit 1221 using the disk that has been

created by the disk key creation unit 1218, and outputs the encrypted title key to the recording unit 1240. Meanwhile the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221, and outputs the re-encrypted C2 content 40 to the recording unit 1240 (lines 25-34, Col. 13). Note that the recording unit 1240 records the audio data that has been transferred from the audio data encryption unit 1223 in an user accessible area in the memory card 1300 and the encrypted disk key and title key in a system area in the memory card 1300 that cannot be accessed by the user (lines 39-43, Col. 13 and Fig. 2 from Harada et al.)). Itkis, Harada et al., and Tatebayashi are analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Itkis with Harada et al. and Tatebayashi since one would have been motivated to (1) provide a production protection system that enables contents to be recorded on a recording medium loaded on a player for replaying contents and the like in order to more intensively protect contents for sale, and enables one of encryption algorithms for distributing contents via the Internet and

for recording contents on the recording medium not to be influenced by the decryption of the other one (lines 53-60, Col. 1 from Harada et al.), and (2) protect the digital productions against unauthorized use when distribute digital productions (lines 17-20, Col. 1 from Tatebayashi). Therefore, it would have been obvious to combine Itkis, Harada et al., and Tatebayashi to obtain the invention as specified in claim 12.

b. Referring to Claims 13 and 27:

As per Claim 13, Itkis, Harada et al., and Tatebayashi disclose the information processing device according to claim 12. In addition, Harada et al. disclose if the decrypting key has not been detected, said decrypting processing means encrypts said decrypting key to store the encrypted decrypting key on the recording medium or in a recording area in the information processing device **[(lines 12-15, 25-29, and 39-43, Col. 13 from Harada et al.)]**, and Itkis discloses said decrypting key calculated using at least one of the node key and the leaf key held in said storage means **[(lines 16-17 and 43-48, Col. 9 and Fig. 2 from Itkis)]**.

As per Claim 27, the rejection of Claim 26 is incorporated. In addition, Claim 27 encompasses limitations that are similar to those of Claim 13. Therefore, it is rejected with the same rationale applied against Claim 13 above.

c. Referring to Claims 14 and 28:

As per Claim 14, Itkis, Harada et al., and Tatebayashi disclose the information processing device according to claim 12 wherein, if the decrypting key has been detected, said decrypting processing means decrypts the decrypting key encrypted using the key unique to each of said information processing devices **[(lines 54-59, Col. 3 and lines 43-48, Col. 9 from Itkis)]**.

As per Claim 28, the rejection of Claim 26 is incorporated. In addition, Claim 28 encompasses limitations that are similar to those of Claim 14. Therefore, it is rejected with the same rationale applied against Claim 14 above.

d. Referring to Claims 26 and 32:

As per Claim 26, Itkis discloses an information processing method used in an information processing device adapted for processing encrypted data, there being a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices, operating as leaves, and a leaf key unique to each of said information processing devices, said method comprising:

retrieving whether or not there is stored a decrypting key used in decrypting said encrypted data **[The content is distributed form, with K denoting the key used for the encryption (K could be a**



**“key-encrypting-key”) (lines 48-50, Col. 1). It is appreciated that a possibility is thus set up for the remainder of the method of FIG. 5 to determine whether the key with which the invalid content key is encrypted is known to the device (lines 47-50, Col. 12 from Itkis). It is further appreciated that a preferably goal of black box analysis is to produce a set of keys which pirate devices do not use for decoding protected content, but which are known to all valid devices (lines 28-31, Col. 13 from Itkis)];**

decrypting the encrypted decrypting key, in case the decrypting key has been detected, to calculate a decrypting key used in decrypting the encrypted data **[performing no more than predetermined number of decryption operations, the predetermined number being the same for all authorized devices, to obtain the content decryption key from an encrypted form thereof, the encrypted form being encrypted with a group key corresponding to a group of which the authorized device is a member (lines 54-59, Col. 3 from Itkis). A key is assigned to each of the groups 100 of FIG. 2. At any point the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K; (if at some point there are g groups in the authorized set 60, g separately encrypted**

**versions preferably are used (lines 43-48, Col. 9 from Itkis)];**

**and**

**decrypting, in case of failure in detecting the decrypting key, a key block formed by key storage data decryptable using at least one of the node key and the leaf key held by said information processing device, to calculate the decrypting key used in decrypting the encrypted data [Accompanying the content is a key block B (the key block can be assumed to include "media key" – e.g., the disc's serial number, etc. (lines 51-53, Col. 1 from Itkis). B can be computed (by the content providers, after examining the pirate devices) in such a way that all non-compromised devices can compute K from B (lines 56-58, Col. 1 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K (lines 41-46, Col. 9 and Fig. 2 from Itkis). Where K is a content encryption key or any other useful key (lines 7-8, Col. 10 from Itkis). Thus, each device 110 need only perform one decryption operation in order to obtain K. It is appreciated that a further, typically fixed number of decryption operations, as is well known in the art, may need**

**to be performed in order to actually obtain protected content (lines 12-16, Col. 10 from Itkis)].**

Itkis does not expressly disclose (1) reading in a table stored on a recording medium or in a storage area in an information processing device, and (2) the decrypting key is stored on said recording medium or in the recording area in said information processing device. However, Tatebayashi discloses (1) reading a table stored on the recording medium or in a storage area in an information processing device **[The encryption key set distribution unit 116 reads the first encryption key set 420 from the encryption key table 114 and writes it into a first encryption key set storage medium (lines 66-67, Col. 8 and line 1, Col. 9)].** In addition, Harada et al. disclose (2) the encrypted decryption key, used for decrypting the content information, is stored on the recording medium **[The title key encryption unit 1222 encrypts the title key that has been created by the title key creation unit 1221 using the disk that has been created by the disk key creation unit 1218, and outputs the encrypted title key to the recording unit 1240. Meanwhile the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221, and outputs the re-**

encrypted C2 content 40 to the recording unit 1240 (lines 25-34, Col. 13). Note that the recording unit 1240 records the audio data that has been transferred from the audio data encryption unit 1223 in an user accessible area in the memory card 1300 and the encrypted disk key and title key in a system area in the memory card 1300 that cannot be accessed by the user (lines 39-43, Col. 13 and Fig. 2)]. Itkis, Harada et al., and Tatebayashi are analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Itkis with Harada et al. and Tatebayashi since one would have been motivated to (1) provide a production protection system that enables contents to be recorded on a recording medium loaded on a player for replaying contents and the like in order to more intensively protect contents for sale, and enables one of encryption algorithms for distributing contents via the Internet and for recording contents on the recording medium not to be influenced by the decryption of the other one (lines 53-60, Col. 1 from Harada et al.), and (2) protect the digital productions against unauthorized use when distribute digital productions (lines 17-20, Col. 1 from Tatebayashi). Therefore, it would have been

obvious to combine Itkis, Harada et al., and Tatebayashi to obtain the invention as specified in claim 26.

As per Claim 32, it is an information recording medium claim corresponding to the method Claim 26. Thus, it is rejected with the same rationale applied against Claim 26 above. In addition, Harada et al. disclose the information recording medium in which the recorded information can be read out **[recording medium that has been set in the recording medium loading unit (lines 47-48, Col. 3 from Harada et al.)]**.

e. Referring to Claim 33:

As per Claim 33, it encompasses some limitations that are similar to those of claim 5. Thus, it is rejected with the same rationale applied against Claim 5 above. In addition, Harada et al. disclose the information recording medium in which the recorded information can be read out **[recording medium that has been set in the recording medium loading unit (lines 47-48, Col. 3 from Harada et al.)]**. Itkis and Harada et al. do not expressly disclose key storage table. However Tatebayashi discloses key table for the encryption key **[The encryption key set distribution unit 116 reads the first encryption key set 420 from the encryption key table 114 (lines 66-67, Col. 8 from Tatebayashi)]**. Itkis, Harada et al., and Tatebayashi are

analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Itkis with Harada et al. and Tatebayashi since one would have been motivated to (1) provide a production protection system that enables contents to be recorded on a recording medium loaded on a player for replaying contents and the like in order to more intensively protect contents for sale, and enables one of encryption algorithms for distributing contents via the Internet and for recording contents on the recording medium not to be influenced by the decryption of the other one (lines 53-60, Col. 1 from Harada et al.), and (2) protect the digital productions against unauthorized use when distribute digital productions (lines 17-20, Col. 1 from Tatebayashi). Therefore, it would have been obvious to combine Itkis, Harada et al., and Tatebayashi to obtain the invention as specified in claim 33.

### **Conclusion**

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
  - a. Dondeti et al. (U.S. Patent 6,240,188) disclose a group key management system and method for providing secure many-to-

many communication is presented. The system employs a binary distribution tree structure. The binary tree includes a first internal node having a first branch and a second branch depending therefrom. Each of the branches includes a first member assigned to a corresponding leaf node. The first member has a unique binary ID that is associated with the corresponding leaf node to which the first member is assigned. A first secret key of the first member is operable for encrypting data to be sent to other members. The first member is associated with a key association group that is comprised of other members. The other members have blinded keys. A blinded key derived from the first secret key of the first member is transmitted to the key association group. Wherein, the first member uses the blinded keys received from the key association group and the first secret key to calculate an unblinded key of the first internal node. The unblinded key is used for encrypting data that is communicated between members located on branches depending from the first internal node.

- b. Ueda et al. (U.S. Patent 6,289,102) disclose an information recording medium includes a lead-in area and a data recording area. Key information is recorded in the lead-in area. Scrambled data is recorded in the data recording area. The scrambled data is descrambled based on the key information. In addition, Ueda et al. disclose the seed key, identification information, master key, disk

Art Unit: 2135


key and title key for descrambling the encrypted content as in Fig.  
20 and 22.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 8:15 to 4:15 M-F. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Yen Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YCS

Feb. 13, 2006

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100